Federal Public Key Infrastructure Policy Authority

FEDERAL PKI POLICY AUTHORITY

July 10, 2012 MEETING MINUTES

GSA
1275 1st St. NE
Conference Room 701A
Washington, DC
9:30 a.m. – 12:00 a.m. EST

9:30	Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
9:35	Discuss / Vote on July 2012 FPKIPA Minutes	Matt King
9:45	Criticality of FPKI Availability - Update	Toby Slusher
10:00	FPKI Management Authority (FPKIMA) Report	Darlene Gore
10:30	FPKI Certificate Policy Working Group (CPWG) Report 1. Discussion/Vote: Delegation of Device Sponsor Responsibilities Change Proposal (Common CP) 2. Discussion/Vote: Common Root CA Offline Operation (Common CP) 3. Discussion: PIV Content Signing Policy Change Proposal 4. Discussion: PIV-I to Non-US Persons Change Proposal 5. Other Updates	Charles Froehlich
11:00	SHA-1 Transition Status	SHA-1 Affiliates
11:10	VA Status Update	John Hancock / Eric Jurasas
11:20	FPKIPA Chair Update	Deb Gallagher

11:30	**Other Agenda Items** ○ *ICAM Update* ○ *If you cannot attend, please designate a proxy* ○ *Next FPKIPA meeting, September 11, 2012*	**Deb Gallagher**
12:00	**Adjourn Meeting**	**Deb Gallagher**

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	O'Brien, Shawn	T
Department of Energy (DOE)	Thomas, Michele	A
Department of Health & Human Services (HHS)	Slusher, Toby	P
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Rice, Barry	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David (Proxy to GSA)	A
Social Security Administration (SSA)	Mitchell, Eric	A
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	T
Veterans Administration (VA)	Miller, Jason	T

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
USPS	Nicholson, Phil	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
FPKIPA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
ExoStar	Baker, George	T
Entrust	Schoen, Isadore	T
GSA FAS	Gore, Darlene	T
DHA (Contractor)	Shomo, Larry	T
CertiPath	Spencer, Judy	P
Treasury (Contractor)	Njadian, Arash	P
SAFE BioPharma	Wilson, Gary	T
State Department (Contractor)	Jung, Jimmy	T
FPKIMA (Contractor, Protiviti)	Louden, Chris	T
FPKIPA (Contractor, Protiviti)	King, Matt	P
Boeing	Knowles, Jacqueline	T
IdenTrust	Cox, Jerry	T
DEA	Rosen, Leo	T
DoD (Contractor, BAH)	Hansom, Maryam	T
DEA (Contractor)	Jain, Amit	T

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at GSA, 1275 1st St. NE, Conference Room 701A, Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:33 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Criticality of FPKI Availability - Update, Toby Slusher

There was no quorum at the beginning of the meeting, so discussion was held about the Criticality of FPKI Availability letter. Mr. Toby Slusher worked with the Tiger Team to finalize the letter, which was distributed to the FPKIPA mail list on August, 10, 2012. Mr. Charles Froehlich commented that the letter seemed to focus on PIV and there is no mention of PKI being used for digital signature, encryption, etc. Mr. Slusher explained that these topics were discussed extensively by the Tiger Team, which agreed that PIV should be the focus of the letter since it was expected that PIV would resonate with the target audience. Ms. Gallagher suggested that the CIOs are most focused on business processes.

The FPKIPA decided that a paragraph would be added to the letter that focuses on PKI uses and its function as a base/infrastructure technology with emphasis on the business flow/work processes (e.g., secure email, signing of documents, better security at physical and logical access points). Mr. Slusher agreed to modify the letter and focus on the business processes first and then address technical details.

Ms. Gallagher noted that this letter is timely because there is a new data call focused on the cost of cyber-security. Mr. Tim Baldridge cited a recent article about the Obama Administration's efforts to improve internet security at large, but Congress has been stalling on the issue since industry is pushing back.

Ms. Gallagher stated that she would mention this letter at the ISIMSC on August 15, 2012 and the ICAMSC on August 22, 2012.

ACTION ITEMS:

1. Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.
2. Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.

Discuss / Vote on July 10, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the July 10, 2012 FPKIPA minutes. HHS motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for July 10, 2012 FPKIPA Minutes			
Voting members	**Vote (HHS Motion; USPS Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)			Absent
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)			Absent
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

FPKI Management Authority (FPKIMA) Report, Darlene Gore

Ms. Wendy Brown presented the FPKIMA Report. Ms. Brown stated that Mozilla discussion about the FPKI had begun. Some positive and negative comments were posted. The negative comments focused on concerns about what information was omitted from the redacted CPS. Ms. Brown responded to the comments providing additional insight about the redactions. FPKIPA members were encouraged to participate in the Mozilla discussion.

Ms. Brown provided an overview of FPKI performance. There have been no unscheduled outages in the last 325 days. LDAP usage went down slightly while HTTP usage went up, and it is expected that this trend will continue as LDAP is phased out. Average response time was .19 seconds and traffic in July 2012 increased by 3% to 1.416 billion requests.

The FPKI TWG will not meet in August 2012 due to membership availability issues. The next meeting will be in September 2012 (EKUs and PDVal to be discussed).

ACTION ITEMS:

1. The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: Delegation of Device Sponsor Responsibilities Change Proposal (Common CP)

Mr. Froehlich presented an overview of the *Delegation of Device Sponsor Responsibilities Change Proposal for the Common CP*. A human device sponsor is responsible for protecting the device's private key and ensuring the certificate is only used for authorized purposes. In many organizations, the persons authorized to sponsor devices (i.e., request the issuance, re-key, modification and revocation of certificates) are managers, not local administrators. These managers may also sponsor multiple devices. This proposed change allows a human device sponsor (who does not physically control the device and/or who lacks sufficient administrative privileges to fulfill these responsibilities) to delegate them to an authorized administrator of the device. The delegation must be documented in writing and signed by both parties. Policy requirements accountability remains with the device sponsor. The CPWG recommended that the FPKIPA move this to a vote.

Ms. Gallagher suggested the FPKI Community should be digitally signing documents similar to those referenced in the change proposal. Mr. Barry Rice, DoS, proposed that the use of digital signatures for PKI-related transactions should be mandatory (i.e., "…must/shall be digitally signed…"). Discussion was held about challenges that still exist with digitally signing of documents (e.g., long-term validation of digital signatures). The FPKIPA requested that the CPWG develop a change proposal to address the issue of digitally-signed documents used in support of PKI operations.

ACTIONS:

1. Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents.

There was a vote to approve the *Delegation of Device Sponsor Responsibilities Change Proposal for the Common CP*. HHS motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for *Delegation of Device Sponsor Responsibilities Change Proposal for the Common CP*			
Voting members	**Vote (HHS Motion; State Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)			Absent
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)			Absent
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

b. Discussion/Vote: Common Root CA Offline Operation (Common CP)

Mr. Froehlich presented an overview of the *Common Root CA Offline Operation Change Proposal for the Common C*P. As the trust anchor for the federal government, the FCPCA root certificate is distributed to relying party applications throughout the government and to the general public via various COTS vendor applications. Vendors are introducing additional requirements for offline operation of CAs to be included in their trust stores. In addition to complying with commercial vendor requirements, operating the FCPCA offline would reduce the opportunities for the FCPCA to be compromised.

Although Common Policy does not explicitly state requirements for FCPCA CRL validity periods or issuance frequencies, this change proposal would allow the FCPCA to be operated in an offline manner with 31-day CRLs, similar to legacy Federal Root CAs. It should be noted that the implementation date is 12-24 months out to allow for planning and pre-implementation actions. Separate discussions will also need to be held regarding the architecture of the FPKI as a result of this change. The CPWG recommended that the FPKIPA move this to a vote.

Mr. Baldridge asked if this change proposal would negate the approval that had been given for the long-term CRL issued by the Legacy Common Policy CA. Ms. Judy Spencer recommended reviewing section 5.8 of the Common Policy CP.

An action was given to the CPWG to review the Common Policy to determine if another change proposal is required.

There was a vote to approve the Change Proposal to allow the Common Policy Root CA to be operated offline with a 31-day CRL. HHS motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for *Common Root CA Offline Operation Change Proposal for the Common CP*			
Voting members	**Vote (HHS Motion; USPS Seconded)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	√		
Department of Energy (DOE)			Absent
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)			Absent

Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)			Absent
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

ACTION:

1. The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA.

c. Discussion: PIV Content Signing Policy Change Proposal

Mr. Froehlich presented an overview of the *PIV Content Signing Policy Change Proposal for the Common CP*. Implementation of this change proposal would create a new PIV Content Signing Policy OID in the Common Policy. Despite objections to additional OIDs, NIST has stated they would reference a PIV Content Signing Policy OID in FIPS 201 if it were included. Currently, FIPS 201-2 requires the “devicesHardware” policy OID plus the PIV Content Signing EKU for certificates issued to CMSs.

Adding a policy OID would provide an opportunity to align with FBCA CP PIV-I policies and define narrower requirements for certificates issued to CMSs used to sign card content. Approval and implementation of this Change Proposal would also depend on whether or not we can convince NIST to allow technical implementation details to be published in the CP and pointed to in FIPS 201 (as we suggested in our comments submitted on August 10, 2012).

Over the next few weeks, the CPWG and FPKI TWG will review the internal effects of this change, and will work to convince NIST to delete most, if not all, PKI technical implementation details from FIPS and replace with pointers to the appropriate FPKI CPs. The time frame for changing FIPS, and even NIST SPs, is too long to accommodate needed changes within the PKI. The FPKIPA needs to decide if it should develop this new policy. If the FPKIPA would like the CPWG to develop the policy, the CPWG recommends an E-Vote once the change proposal is finalized by the CPWG very soon.

The benefits of having such a policy were discussed (e.g., tighter controls over issuance of content signing certificates, alignment of FBCA and Common policies).

The FPKIPA agreed that the change proposal was needed, and directed the CPWG to finalize the change proposal.

ACTIONS:

1. Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.

d. Discussion/Vote: PIV-I to Non-US Persons Change Proposal

Mr. Froehlich presented an overview of the *PIV-I to Non-US Persons Change Proposal*. CertiPath has proposed a change based on a situation that at least some of their members are encountering: the need for PIV-I like credentials issued to non-U.S. citizens overseas by non-U.S. PIV-I providers, for use primarily outside the U.S. to predominantly access other than U.S. facilities and networks. Essentially, foreign providers are looking to establish a PIV-I like infrastructure and credentials for their own use that might also be acceptable for use within the U.S.

This issue is of interest to the FPKI because (a) CertiPath is a designated PIV-I provider; and, (b) CertiPath is a co-equal member of the 4 Bridges Forum, sharing mutual cross-certification with the FBCA. This may be an opportunity to set a global gold standard for PKI. This topic resulted in extensive discussion, and additional changes beyond those already suggested were proposed. The CPWG will continue discussions over the next few weeks.

e. Other Updates

1. DoD Application for Cross Certification

DoD has submitted an application for cross-certification for a new CA that will operate with SHA-2. The CPWG discussed the mapping process and comments to the application, which was required due to the addition of the SHA-2 CA infrastructure. It was determined that there are two issues involved: (1) the normal CP-to-CP mapping, compliance auditing, and operational testing that are part of any cross-certification application; and, (2) the need to discuss the DoD architecture especially in relation to the FPKI architecture. The CPWG requests that the FPKIPA take the necessary approval action on the DoD cross-certification application in accordance with the Criteria and Methodology document.

It was agreed that an E-Vote would be held after the meeting. The results of the E-Vote are as follows:

Approval Vote for DoD Cross-Certification Application			
Voting members	**Vote**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)			Abstain
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC)			Absent
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)	√		
Veterans Administration (VA)	√		

2. **FIPS 201-2 Final Comments**

The CPWG went through the *Comments and Disposition* document to review the FPKI comments that were declined. Three comments were submitted to the FIPS 201 team: (1) proposing deferring technical details to the Common Policy; (2) allowing PIV-I chain of trust data to be used to meet PIV registration requirements; and (3) Including a reference to the PIV content signing policy. No FPKI action on any item was recommended, with the exception of identifying the future need to lobby OMB to modify Memorandum M-05-24 to permit broader acceptance of PIV-I to eliminate the need to issue duplicate credentials to contractor personnel.

3. **Use of PIV Card for requesting equal or lower level certificates**

This Change Proposal had been introduced previously and issues had been identified. DHS will develop revised language for presentation at a future CPWG meeting.

SHA-1 Transition Status, SHA-1 Affiliates

Mr. King asked for updates from Affiliates who are transitioning to SHA-1. No updates were provided.

ACTION ITEMS:

1. Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.

VA Status Update, John Hancock / John Hancock, Eric Jurasas

Mr. Jason Miller stated that there was no update except that remediation updates are continuing. Mr. Miller mentioned that Mr. Eric Jurasas has taken over the VA PIV program, so Mr. Miller will work to obtain more detailed information.

ACTION ITEMS:

1. Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.

FPKIPA Chair Update, Deb Gallagher

Upcoming meetings and events:

Meeting	Date
Strong Logical Access Tiger Team (SLATT)	Wednesdays 10:00 – 11:00am
ISIMSC	August 2012
CPWG	August 21, 2012
IAB	August 22, 2012
ICAMSC	August 22, 2012
IA Symposium (Nashville, TN)	August 28 – 30, 2012
ACAG Industry Day	Sept. 5, 2012
FPKI TWG	Sept 18, 2012 (August 2012 cancelled due to lack of member availability)

The SLATT metrics will be completed by the end of August 2012. Ms. Gallagher will also resubmit the metrics related to the FPKI Security Profile to the FISMA team.

During the August 15, 2012 ISIMC meeting, the work for next year will be discussed. A new working group focused on mobility has been established. The ICAMSC (10am-12pm) and IAB (1-3 pm) will be held at GSA on August 22, 2012. The NSTIC Workshop will be held in Chicago on August 15-16, 2012.

Ms. Gallagher had staff review the new NIST SP 800-157 Doc on mobile devices

The Trust Framework Provider adoption process is being revised. It will now include PKI (i.e., PIV-I) not just LOA 1, 2, and 3 non-PKI.

The NSS IdAM WG is currently conducting a gap analysis of FICAM and IDAM in the Secret fabric. They will develop a report based on the analysis, and DHS has been asked to develop an implementation plan for closing the gaps and helping them align with FICAM.

The Federal Cloud Credentialing Service (FCCX) is moving forward and will be a Middleware service to provide the credential service for citizen authentication to federal sites. An industry day was held last week to find out what industry best practices are available for federation. USPS is very interested in providing the service.

The next FPKIPA meeting is September 11, 2012 at USPS.

ACTION:

1. Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team.

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 11:57 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSs	Wendy Brown	8-May-12	30-Jul-12	Open
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Open
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Open
467	Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.	Toby Slusher	14-Aug-12	11-Sep-12	Open
468	Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.	Deb Gallagher	14-Aug-12	30-Sep-12	Open
469	The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.	Wendy Brown	14-Aug-12	11-Sep-12	Open
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Open
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
472	Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.	Charles Froehlich	14-Aug-12	11-Sep-12	Open

Number	Action Statement	POC	Start Date	Target Date	Status
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open
474	Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.	Jason Miller	14-Aug-12	11-Sep-12	Open
475	Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team	Deb Gallagher	14-Aug-12	11-Sep-12	Open